AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. – 11. (Cancelled)

11. (New) A method for protecting a datum, wherein the datum is encrypted and, prior to sending the datum to a recipient, the datum is divided into at least a first block and a second block, the method comprising:

receiving, at the recipient, the first block;

decrypting the first block to obtain a decrypted first block;

re-encrypting the decrypted first block to obtain a re-encrypted first block using an encryption algorithm, prior to decrypting the second block;

receiving, at the recipient, the second block;

decrypting the second block to obtain a decrypted second block; and

re-encrypting the decrypted second block to obtain a re-encrypted second block using the encryption algorithm,

wherein the first block and the second block are transmitted individually to the recipient.

12. (New) The method of claim 11, further comprising:

analyzing the decrypted first block to determine whether the decrypted first block comprises a first non-useful datum;

if the decrypted first block comprises the first non-useful datum:

extracting the first non-useful datum from the decrypted first block to obtain a modified decrypted first block;

re-encrypting the modified decrypted first block to obtain a modified re-encrypted first block prior to decrypting the second block, wherein the modified decrypted first block is re-encrypted instead of the decrypted first block.

13. (New) The method of claim 12, further comprising:

analyzing the decrypted second block to determine whether the decrypted second block comprises a second non-useful datum;

if the decrypted second block comprises a second non-useful datum:

extracting the second non-useful datum from the decrypted first block to obtain a modified decrypted second block;

re-encrypting the modified decrypted second block to obtain a modified re-encrypted second modified block, wherein the modified decrypted second block is re-encrypted instead of the decrypted second block.

14. (New) The method of claim 12, wherein the first non-useful datum comprises at least one selected from the group consisting of padding, a tag associated with the datum, a header associated with the datum, a header associated with the first block, a length associated with the decrypted first block, and a length associated with the datum.

15. (New) The method of claim 11, further comprising:

concatenating the re-encrypted second block with the re-encrypted first block to obtain re-encrypted datum.

16. (New) The method of claim 11, wherein the decrypted first block is segmented into a first segment and a second segment prior to being re-encrypted, wherein a length of first segment correspond is equal to a required segment size of the encryption algorithm and a length of the second segment is equal to a required segment size of the encryption algorithm.

17. (New) The method of claim 11, wherein the recipient is a smart card.

18. (New) A smart card configured to:

receive a first block;

decrypt the first block to obtain a decrypted first block;

re-encrypt the decrypted first block to obtain a re-encrypted first block using an encryption algorithm, prior to decrypting a second block;

receive the second block;

decrypt the second block to obtain a decrypted second block; and

re-encrypt the decrypted second block to obtain a re-encrypted second block using the encryption algorithm,

wherein a datum is encrypted and, prior to sending the datum to the smart card, the datum is divided into at least a first block and a second block, and

wherein the first block and the second block are transmitted individually to the smart card.

19. (New) A method for protecting a datum, wherein the um is encrypted and, prior to sending the datum to a recipient, the datum is divided into at least a first block and a second block, the method comprising:

receiving, at the recipient, the first block;

decrypting the first block to obtain a decrypted first block;

segmenting the decrypted first block into a first segment and a second segment, wherein a length of the first segment is equal to a required segment size of an encryption algorithm;

re-encrypting the first segment, using the encryption algorithm, to obtain a re-encrypted first segment, prior to decrypting the second block;

re-encrypting the second segment, using the encryption algorithm, to obtain a re-encrypted second segment prior to decrypting the second block, if a length of the second segment is equal to the required segment size of the encryption algorithm;

receiving, at the recipient, the second block;

decrypting the second block to obtain a decrypted second block;

if the length of the second segment is less than the required segment size of the encryption algorithm:

combining the decrypted second block with the second segment to obtain a decrypted concatenated block; and

re-encrypting the decrypted concatenated block using the encryption algorithm;

if the length of the second segment is equal to the required segment size of the encryption algorithm:

re-encrypting the decrypted second block to obtain a re-encrypted second block using the encryption algorithm,

wherein the first block and the second block are transmitted individually to the smart card.

20. (New) The method of claim 19, further comprising:

prior to segmenting the first decrypted block:

analyzing the decrypted first block to determine whether the decrypted first block comprises a first non-useful datum;

if the decrypted first block comprises the first non-useful datum:

extracting the first non-useful datum from the decrypted first block to obtain a modified decrypted first block;

segmenting the modified decrypted first block into a third segment and a fourth segment, wherein a length of the third segment is equal to a required segment size of the encryption algorithm, wherein the modified first decrypted block is segmented instead of the decrypted first block and wherein the third and fourth segments are generated instead of the first and second segments;

re-encrypting the third segment, using the encryption algorithm, to obtain a re-encrypted third segment prior to decrypting the second block; and

re-encrypting the fourth segment, using the encryption algorithm, to obtain a re-encrypted fourth segment prior to decrypting the second block, if a length of the fourth segment is equal to the required segment size of the encryption algorithm.

21. (New) The method of claim 19, wherein re-encrypting the decrypted concatenated block comprises:

segmenting the decrypted concatenated block in to a third segment and fourth segment;

re-encrypting the third segment if length of the third segment is equal to the required segment size of an encryption algorithm; and

re-encrypting the fourth segment if length of the fourth segment is equal to the required segment size of an encryption algorithm.

22. (New) A smart card configured to:

receive a first block;

decrypt the first block to obtain a decrypted first block;

segment the decrypted first block into a first segment and a second segment, wherein a length of the first segment is equal to a required segment size of an encryption algorithm;

re-encrypt the first segment, using the encryption algorithm, to obtain a re-encrypted first segment, prior to decrypting a second block;

re-encrypt the second segment, using the encryption algorithm, to obtain a re-encrypted second segment prior to decrypting the second block, if a length of the second segment is equal to the required segment size of the encryption algorithm;

receive the second block;

decrypt the second block to obtain a decrypted second block;

if the length of the second segment is less than the required segment size of the encryption algorithm:

combine the decrypted second block with the second segment to obtain a decrypted concatenated block; and

re-encrypt the decrypted concatenated block using the encryption algorithm;

if the length of the second segment is equal to the required segment size of the encryption algorithm:

re-encrypt the decrypted second block to obtain a re-encrypted second block using the encryption algorithm,

wherein a datum is encrypted and, prior to sending the datum to the smart card, the datum is divided into at least the first block and the second block, and

wherein the first block and the second block are transmitted individually to the smart card.

23. (New) A method for protecting a datum, wherein the data is encrypted and, prior to sending the datum to a recipient, the datum is divided into at least a first block and a second block, the method comprising:

receiving, at the recipient, the first block;

inverting the first block to obtain a first inverted block;

decrypting the first inverted block to obtain a decrypted first inverted block;

determining a first amount of padding to append to the decrypted first inverted block;

appending the first amount of padding to the decrypted first inverted block to obtain a padded decrypted first inverted block;

re-encrypting the padded decrypted first inverted block to obtain a re-encrypted first inverted block using an encryption algorithm, prior to decrypting the second block;

receiving, at the recipient, the second block;

inverting the second block to obtain an inverted block;

decrypting the second inverted block to obtain a decrypted second inverted block; and

re-encrypting the decrypted second inverted block to obtain a re-encrypted second inverted block using the encryption algorithm,

wherein the first block and the second block are transmitted individually to the recipient.

24. (New) The method of claim 23, further comprising:

analyzing the decrypted first inverted block to determine whether the decrypted first inverted block comprises a first non-useful datum;

if the decrypted first inverted block comprises the first non-useful datum:

extracting the first non-useful datum from the decrypted first inverted block to obtain a modified decrypted first inverted block;

re-encrypting the modified decrypted first inverted block to obtain a re-encrypted first inverted block prior to decrypting the second block, wherein the modified decrypted first inverted block is re-encrypted instead of the decrypted first inverted block.

25. (New) The method of claim 23, further comprising:

pre-pending the re-encrypted second inverted block to the re-encrypted first inverted block.

26. (New) A smart card configured to:

receive a first block;

invert the first block to obtain a first inverted block;

decrypt the first inverted block to obtain a decrypted first inverted block;

determine a first amount of padding to append to the decrypted first inverted block;

append the first amount of padding to the decrypted first inverted block to obtain a padded decrypted first inverted block;

re-encrypt the padded decrypted first inverted block to obtain a re-encrypted first inverted block using an encryption algorithm, prior to decrypting a second block;

receive the second block;

invert the second block to obtain an inverted block;

decrypt the second inverted block to obtain a decrypted second inverted block; and

re-encrypt the decrypted second inverted block to obtain a re-encrypted second inverted block using the encryption algorithm,

wherein a datum is encrypted and, prior to sending the datum to the smart card, the datum is divided into at least the first block and the second block, and

wherein the first block and the second block are transmitted individually to the smart card.

27. (New) A method for protecting the datum, wherein the datum is encrypted and, prior to sending the datum to a recipient, the datum is divided into at least a first block and a second block, the method comprising:

receiving, at the recipient, the first block;

inverting the first block to obtain a first inverted block;

decrypting the first block to obtain a decrypted first inverted block;

segmenting the decrypted first inverted block into a first segment and a second segment, wherein a length of the first segment is equal to a required segment size of an encryption algorithm;

re-encrypting the first segment, using the encryption algorithm, to obtain a re-encrypted first segment, prior to decrypting a second inverted block;

re-encrypting the second segment, using the encryption algorithm, to obtain a re-encrypted second segment prior to decrypting a second inverted block, if a length of the second segment is equal to the required segment size of the encryption algorithm;

receiving the second block;

inverting the second block to obtain the second inverted block;

decrypting the second inverted block to obtain a decrypted second inverted block;

if the length of the second segment is less than the required segment size of the encryption algorithm:

combining the decrypted second inverted block with the second segment to obtain a decrypted concatenated block; and

re-encrypting the decrypted concatenated block using the encryption algorithm;

if the length of the second segment is equal to the required segment size of the encryption algorithm:

re-encrypting the decrypted second inverted block to obtain a re-encrypted second block using the encryption algorithm,

wherein the first block and the second block are transmitted individually to the recipient.

28. (New) The method of claim 27, further comprising:

prior to segmenting the first decrypted inverted block:

analyzing the decrypted first inverted block to determine whether the decrypted first block comprises a non-useful datum;

if the decrypted first block comprises the non-useful datum:

extracting the non-useful datum from the decrypted first inverted block to obtain a modified decrypted first inverted block;

segmenting the modified decrypted inverted first block into a third segment and a fourth segment, wherein a length of the third segment is equal to a required segment size of the encryption algorithm, wherein the modified first decrypted block is segmented instead of the decrypted first inverted block and wherein the third and fourth segments are generated instead of the first and second segments;

re-encrypting the third segment, using the encryption algorithm, to obtain a re-encrypted third segment prior to decrypting the second inverted block; and

re-encrypting the second segment, using the encryption algorithm, to obtain a re-encrypted fourth segment prior to decrypting the second inverted block, if a length of the fourth segment is equal to the required segment size of the encryption algorithm.

29. (New) The method of claim 27, wherein combining the decrypted second inverted block with the second segment comprises pre-pending the decrypted second inverted block to the second segment.

30. (New) A smart card configured to:

receive a first block;

invert the first block to obtain a first inverted block;

decrypt the first block to obtain a decrypted first inverted block;

segment the decrypted first inverted block into a first segment and a second segment, wherein a length of the first segment is equal to a required segment size of an encryption algorithm;

re-encrypt the first segment, using the encryption algorithm, to obtain a re-encrypted first segment, prior to decrypting a second inverted block;

re-encrypt the second segment, using the encryption algorithm, to obtain a re-encrypted second segment prior to decrypting a second inverted block, if a length of the second segment is equal to the required segment size of the encryption algorithm;

receive the second block;

invert the second block to obtain the second inverted block;

decrypt the second inverted block to obtain a decrypted second inverted block;

if the length of the second segment is less than the required segment size of the encryption algorithm:

combine the decrypted second inverted block with the second segment to obtain a decrypted concatenated block; and

re-encrypt the decrypted concatenated block using the encryption algorithm;

if the length of the second segment is equal to the required segment size of the encryption algorithm:

re-encrypt the decrypted second inverted block to obtain a re-encrypted second block using the encryption algorithm,

wherein a datum is encrypted and, prior to sending the datum to the smart card, the datum is divided into at least the first block and the second block, and

wherein the first block and the second block are transmitted individually to the smart card.